

UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia



In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Case No. 3:18SW48

One Hitachi Hard Drive S/N MS2DDLKS, containing
encrypted image files for Western Digital HD S/N
WCASYD69, & Western Digital HD S/N WMASU027363

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

One Hitachi Hard Drive S/N MS2DDLKS located at FBI, 1970 E Parham Rd, Richmond, VA, which is more particularly described in Attachment A of the attached Affidavit and hereby incorporated by reference as if fully stated herein.

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):

See Attachment B of the attached Affidavit, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. §§ 2251 and 2252 Production and Possession of Child Pornography

The application is based on these facts:

See attached Affidavit, incorporated herein by reference.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

[Signature]
Applicant's signature

Melvin Gonzalez, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 03/06/2018

City and state: Richmond, VA

IS/
David J. Novak
United States Magistrate Judge
Judge's signature

David J. Novak, United States Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF:
One Hitachi Hard Drive, S/N MS2DDLKS,
containing encrypted image files for 92-
227.00002.B (a Western Digital 640GB Hard
Drive, Model WD6400, S/NWCASYD691611)
and 92-227.00002.C (a Western Digital 320GB
External Hard Drive, Model WD3200, S/N
WMASU0273630)

Case No. _____

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Melvin Gonzalez, having been first duly sworn, do hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent of the Federal Bureau of Investigation (FBI), United States Department of Justice, and have been so employed by the FBI for over eleven years. I am currently assigned to the Richmond Field Office, Richmond, VA. I am assigned to the Child Exploitation Task Force (CETF) which conducts investigations pertaining to child sex trafficking, child pornography, and child abductions. I have received training from the FBI in the areas of child exploitation. I was previously assigned for three years to the San Juan Field Office, where I investigated violent crimes, gangs, and drug trafficking. During my career in law enforcement, I have received extensive training in the conduct of a variety of investigations, including drug investigations, organized crime, violent crime, white collar crime, and others. In my experience, I have participated in a wide range of investigations. That experience has

included receiving and analyzing information, conducting interviews, collecting and processing physical evidence, and preparing evidence for trial.

2. In the course of my employment as a sworn law-enforcement officer, I have participated in the execution of numerous search warrants resulting in the seizure of computers, magnetic storage media for computers, other electronic media, and other items evidencing violations of state and federal laws, including various sections of Title 18, United States Code §§ 2251, Title 18 U.S.C. § 2422 (enticement or coercion of a minor to engage in illegal sexual activity) and Title 18 U.S.C. § 2252, involving child exploitation and child pornography offenses.

3. The statements contained in this affidavit are based in part on: information provided by FBI Special Agents, FBI Task Force Agents, and other law-enforcement officers; written reports about this and other investigations that I have received, directly or indirectly, from other law-enforcement agents; information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law-enforcement agents; independent investigation and analysis by FBI agents/analysts and computer forensic professionals; and my experience, training, and background as a Special Agent with the FBI. Because this affidavit is being submitted for the limited purpose of securing authorization for the requested search warrant, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish the necessary foundation for the requested warrant.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. I have probable cause to believe that the property to be searched, one Hitachi Hard Drive S/N MS2DDLKS, containing encrypted image files for 92-227.00002.B (a Western Digital

640GB Hard Drive, Model WD6400, Serial Number WCASYD691611) and 92-227.00002.C (a Western Digital 320GB External Hard Drive, Model WD3200, Serial Number WMASU0273630), hereinafter referred to as the DEVICES, contain contraband and evidence of a crime, fruits of a crime, and instrumentalities of violations of: 18 U.S.C. § 2251 (production of child pornography) and 18 U.S.C. § 2252 (possession of, knowing access or attempted access with intent to view, child pornography). I submit this application and affidavit in support of a search warrant authorizing a search of the DEVICES, as further described in Attachment A which is incorporated herein by reference, which is located in the Eastern District of Virginia. Located within the DEVICES to be searched, I seek to seize evidence, fruits, and instrumentalities of the foregoing criminal violations.

5. The applied-for warrant would authorize the forensic examination of the DEVICES for the purpose of identifying electronically-stored data particularly described in Attachment B.

DEFINITIONS

6. The following definitions apply to this Affidavit and attachments hereto:
- a. “**Erotica**,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, legally obscene or that do not necessarily depict minors in sexually explicit conduct.
 - b. “**Child Pornography**,” as used herein, is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image

that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

- c. **Visual depictions** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which are capable of conversion into a visual image, and data which are capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. See 18 U.S.C. § 2256(5).
- d. **Minor** means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).
- e. **Sexually explicit conduct** means actual or simulated: (i) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

TECHNICAL TERMS

7. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. **“Computer,”** as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction

with such device.”

- b. **“Computer Server”** or **“Server,”** as used herein is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user’s computer via the Internet. A domain name system (“DNS”) server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser.

Essentially, the domain name must be translated into an Internet Protocol (“IP”) address so the computer hosting the web site may be located, and the DNS server provides this function.

- c. **“Computer hardware,”** as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

- d. **“Computer software,”** as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- e. **Wireless telephone:** A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- f. **Digital camera:** A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a

variety of fixed and removable storage media to store their recorded images.

Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- g. **Portable media player:** A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- h. **GPS:** A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite

contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- i. **Tablet:** A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, which is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.
- j. The "**Internet**" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- k. "**Internet Service Providers**" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to

the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line ("DSL") or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider ("ISP") over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

- l. **"Internet Protocol address"** or **"IP address"** refers to a unique number used by a computer to access the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- m. The terms **"records," "documents,"** and **"materials,"** as used herein, include all

information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

8. On or about June 12, 2017, the CETF for the FBI Richmond Division received a complaint regarding a possible child pornography production matter.

9. The Louisiana Bureau of Investigation Cybercrime Unit (LBICU) advised that on May 27, 2016, they received several cyber tips from the National Center for Missing and Exploited Children regarding possible possession of child pornography. After conducting their investigation, officers with the LBICU executed a search warrant on June 2, 2016, at 244 Olivier St., New Orleans, Louisiana. While executing the warrant, agents made contact with Alexander Witt, DOB: 09/28/1988. During the search of the residence, agents located and seized several devices to include the following:

- a. One Black Window Tablet (0025B-70156-70156-78077-AAOEM);
- b. One Western Digital Hard Drive, Model WD6400, S/N WCASYD691611;
- c. One HTC 626S, IMEI: 3572006240713;
- d. One Western Digital External Hard Drive, Model WD3200, S/N
WMASU0273630.

10. Agents also interviewed Witt who advised that that he had access to and downloaded child pornography several times to include while he resided in Virginia. Witt was subsequently charged with possession of child pornography in Louisiana.

11. On June 9, 2017, officers from the LBICU met with a computer forensic examiner in order to review images located in some of the devices seized during the search of Witt's residence. According to the officers' reports, thousands of child pornography images were located during the forensic exam of the two Western Digital Hard Drives referenced above.

12. Also during the exam, officers identified two folders saved onto the Western Digital Hard Drives labeled "Halloween 08" and "Halloween 09." Several images in these folders show Witt in a costume along with several juveniles, also in costumes. Also located on the Western Digital Hard Drives was a folder labeled "Alyssa" that contained images of a minor, white female posing nude with the camera angle focused on her genitals. Upon reviewing images from both folders, officers determined that the images of the nude juvenile and the juvenile female from the "Halloween" photos depicted the same person.

13. During their investigation, LBICU officers learned that Witt most likely resided in Virginia when these images were taken, and thus the images were transported interstate to Louisiana. LBICU provided a copy of the forensic extraction images located in the "Alyssa"

folder to the FBI Richmond CETF.

14. On June 22, 2017, FBI Richmond CETF agents identified the young female from the “Alyssa” file, (hereinafter “V1”). V1, who is now an adult, was located in Chesterfield County, Virginia. On July 5, 2017, an FBI Child Adolescent Forensic Interviewer (CAFI) interviewed V1. During the interview, the interviewer displayed some of the above referenced images recovered from the Western Digital Hard Drives, and V1 subsequently identified herself as the subject of the images. Specifically, these images were located in the “Alyssa” folder saved onto the hard drives. V1 displayed extreme emotional trauma from the sexual abuse. She then provided details of the sexual abuse and advised that her cousin (hereinafter “V2”) was also sexually assaulted by Witt. V1 advised that Witt sexually assaulted them at the same time while he recorded it on video. Both V1 and V2 were minors when these acts occurred.

15. On July 10, 2107, FBI Agents identified and contacted V2 via phone and scheduled a forensic interview. V2, who is now 20 years old, resided in Greendale, Indiana during that time.

16. On July 19, 2017, a LBICU computer forensic examiner identified “thumbcache” images of child pornography that most likely depicted V1 and V2 in sexual acts. Some of the images have date stamps of “07/18/2010,” “12/23/2010” and “09/19/2011,” when V1 and V2 were approximately 12 to 14 years old. LBICU provided the images to the FBI CETF. Several of these images were used during the forensic interview of V2.

17. On August 4, 2017, a FBI CAFI interviewed V2. V2 advised that her abuse by Witt began when she was approximately 7 or 8 years-old and lasted until she was approximately 14 years-old. Witt forced her to engage in sexual acts with him and would take photos and videos of the acts. Witt threatened to tell V2’s grandmother and also threatened to kick her out of the

residence naked. V2 recalls that when she was approximately 8 years-old she refused to engage in sex and Witt kicked her out of the residence naked.

18. V2 also corroborated that Witt sexually assaulted V1 and V2 at the same time and recorded the acts. Witt threatened to tell V2's grandmother and gave them alcoholic drinks. V1 and V2 were also approximately 10 to 14 years-old when Witt forced them to engage in sex with each other. V2 recalls several electronic devices used by Witt to record the sexual encounters and also recalls finding a hidden CD with what appeared to be a back-up of the recorded sexual encounters.

19. V2 advised that Witt continued to sexually approach her in subsequent years but she refused. V2 recalls that Witt sexually approached her in April, 2017 when V2 was visiting her grandmother and Witt was residing there on bond.

20. V2 is also aware that Witt has also sexually approached V1 recently and has requested nude images of her. V2 is aware that Witt's mother located some of these recent images in Witt's phone.

21. On October 25, 2017, your affiant received via FedEx a Hitachi Hard Drive S/N MS2DDLKS from the LBICU, which contained encrypted image files for 92-227.00002.B and 92-227.00002.C (DEVICES), pertaining to Alexander Witt. The Hitachi hard drive S/N MS2DDLKS, containing encrypted image file for 92-227.00002.B (Western Digital 640GB Hard Drive, Model WD6400, Serial Number WCASYD691611) and 92-227.00002.C (Western Digital 320GB External Hard Drive, Model WD3200, Serial Number WMASU0273630) (DEVICES), was placed in the Control Evidence Room, CART Room, Shelf 10, Bin 1, at the Richmond FBI Office, 1970 E. Parham Road, Richmond, Virginia.

22. This search warrant seeks permission to search the Hitachi Hard Drive S/N MS2DDLKS, containing encrypted image files for 92-227.00002.B (Western Digital 640GB Hard Drive, Model WD6400, Serial Number WCASYD691611) and 92-227.00002.C (Western Digital 320GB External Hard Drive, Model WD3200, Serial Number WMASU0273630) (DEVICES) using additional forensic extraction tools in order to collect evidence pertaining to the production and possession of child pornography.

CHARACTERISTICS OF COLLECTORS OF CHILD PORNOGRAPHY

22. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereafter “collectors”).

23. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.

24. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature and sexual aids.

25. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.

26. Collectors almost always possess and maintain their “hard copies” of child pornographic images and reference materials (*e.g.*, mailing and address lists) in a private and secure location. With the growth of the Internet and computers, a large percentage of most collections today are in digital format. Typically, these materials are kept at the collector’s residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods, even for years. Collectors often discard child pornography images only while “culling” their collections to improve their overall quality.

27. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.

28. Collectors prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

29. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation

between subscription and collection behavior has been repeatedly confirmed during nationwide law enforcement initiatives.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

30. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

31. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In

addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

32. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

33. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would

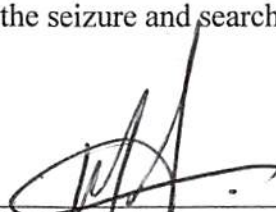
authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

SPECIFICITY OF SEARCH WARRANT RETURN

34. Consistent with the Court's current policy, the search warrant return will list the model(s) and serial number(s) of the DEVICES. Additionally, the search warrant return will include the total numbers of each type of digital media that has been seized searched (*e.g.*, "ten (10) 3.5" diskettes; twenty (20) CDs; twenty (20) DVDs; three (3) USB drives; one (1) 256 MB flash memory card," etc.).

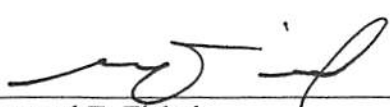
CONCLUSION

35. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located in the DEVICES described in Attachments A. I respectfully request that this Court issue a search warrants for the DEVICES, authorizing the seizure and search of the items described in Attachment B



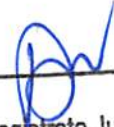
Melvin Gonzalez
Special Agent
Federal Bureau of Investigation

SEEN AND APPROVED BY:



Samuel E. Fishel
Special Assistant United States Attorney

Sworn to me this 6th day of March, 2018



David J. Novak
United States Magistrate Judge
David J. Novak
UNITED STATES MAGISTRATE JUDGE

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Richmond Division

ATTACHMENT A

The property to be searched is:

- 1- One Hitachi Hard Drive S/N MS2DDLKS, containing encrypted image files for 92-227.00002.B (Western Digital 640GB Hard Drive, Model WD6400, Serial Number WCASYD691611) and 92-227.00002.C (Western Digital 320GB External Hard Drive, Model WD3200, Serial Number WMASU0273630). The DEVICES are currently located at the FBI Richmond Field Office, 1970 E. Parham Road, Richmond, Virginia, Evidence Control Room.

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Richmond Division

ATTACHMENT B

EVIDENCE TO BE SEIZED

1. All records on the Device described in Attachment A that relate to violations of 18 U.S.C. §§ 2251 and 2252.
 - a. Any and all visual depictions of minors;
 - b. Any and all address books, names, and lists of names and addresses of minors;
 - c. Any and all diaries, notebooks, notes, and any other records reflecting physical contact, whether real or imagined, with minors, and any such items discussing sexual activities with minors;
 - d. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids;
 - e. Records relating to the email accounts
 - f. Evidence of who used, owned, or controlled the DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - g. records of or information about Internet Protocol addresses used by the DEVICES;
 - h. records of or information about the DEVICES' Internet activity, including

firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

- i. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.